

## Remarks

Claims 1-63 are pending.

The Examiner rejected Claims 1-63 under 35 U.S.C. § 103(a) as being unpatentable over the article "Fast Inter-AP Handoff using Predictive Authentication Scheme in a Public Wireless Network." ("Choi"). With respect to Claim 1, the Examiner states:

C1. A method for handoff in a wireless communication network, comprising: Generating a handoff encryption key [Page 1, Introduction, line 11-14] handing off a wireless terminal from a first access point to a second access point [Page 1, Introduction, Lines 11-14]; and communicating data packets, between the second access point and the wireless terminal [Page 1, Introduction, Lines 11-14, page 6, 3.2 lines 8-15, page 7, Fig. 5, 6]. Choi teaches the re-authentication after handoff as shown in Fig. 6. Choi doesn't expressly mention communication data packets encrypted with the handoff encryption key, between the second access point and the wireless terminal for immediate secured data transmission (i.e., secure data transmission during the handoff without perceivable interruption).

Faccin teaches communicating data packets encrypted with the handoff encryption key, between the second access point and the wireless terminal for immediate secured data transmission (secure data transmission during the handoff without perceivable interruption i.e. before the authentication of the wireless terminal) [col. 2 lines 1-16, Fig. 1, 5]

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Faccin with Choi, since one would have been motivated to provide security mobility between two cellular systems [Faccin col. 1 lines 9-10].

Applicants respectfully traverse the Examiner's rejection. As the Examiner noted, Claim 1 recites a method by which secured data communication is carried out immediately upon handoff and before authentication is complete:

1. A method for handoff in a wireless communication network, comprising:

generating a handoff encryption key;  
handing off a wireless terminal from a first  
access point to a second access point; and

initiating authentication of the wireless terminal  
with an authentication server and communicating data  
packets encrypted with the handoff encryption key  
between the second access point and the wireless  
terminal for immediate secured data transmission before  
authentication of the wireless terminal is completed.

As explained in Applicants' Specification, at page 15, paragraphs [0060]-[0063], the above-underscored limitations allows data communication during the handoff without perceivable interruption due to the latency of authentication with an authentication server. The above underscored limitations are, however, neither disclosed nor suggested by Choi or Faccin. Specifically, Choi teaches against authentication with an authentication server at the second access point:

Fig. 6 shows the case of re-authentication after handoff. When the mobile host hands off to any other AP, since the new AP receives session information in advance, further message exchanges are not needed. The relocated mobile host can obtain all information from the new AP and it is not necessary to send an "Access Request" request to the AAA server. Generally, since the AAA server is often located in a remote domain for more scalable service, the delay in the path from the AP to the AAA server is a critical server in the total handoff latency. All of these functions can be implemented by using various attributes available in the current AAA protocol.

(Choi, at page 7, lines 7-15)

Likewise, Faccin does not teach at col. 2, lines 1-16, nor in Figs. 1 and 5, authentication with an authentication server at the second access point:

generating one or more second ciphering keys for a second cellular system where the one or more second ciphering keys are generated by an interoperability authentication center at a first cellular system and by a mobile device separately; encrypting traffic between the mobile device and the first cellular system using one or more first ciphering keys for the

first cellular system; approving a handoff of the traffic of the mobile device from the first cellular system to the second cellular system; sending the one or more second ciphering keys from the first cellular system to the second cellular system; and performing handoff by the mobile device from the first cellular system to the second cellular system where traffic between the mobile device and the second cellular system is encrypted using the one or more second ciphering key. Ciphering of the traffic is maintained during handoff.

Therefore, the combined teachings of Choi and Faccin do not meet the limitations of amended Claim 1. Accordingly, Claim 1 and its dependent Claims 2-27 are each allowable over the combined teachings of Choi and Faccin. Similarly, independent Claims 28, 34, 41, 49, 55-56, and 63 -- which each also recite secured data communication using a handoff encryption key occurs while an authentication process is being carried out and before completion of the authentication -- and their respective dependent Claims 29-33, 35-40, 41-48, 50-52, are each allowable over the combined teachings of Choi and Faccin.

Claims 53-54 and 57-62 each recite a specific algorithm for generating a handoff encryption key -- i.e., using "an address of the wireless terminal" or "an open parameter" with a "secret parameter." Such an algorithm is neither disclosed nor suggested by Choi or Faccin. Accordingly, Claims 53-54 and 57-62 are also each allowable over the combined teachings of Choi and Faccin.

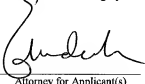
Accordingly, reconsideration and allowance of Claims 1-63 are requested.

The Examiner provisionally rejected Claims 1-63 under the doctrine of non-statutory obviousness-type double patenting over Claims 1-25 of U.S. patent application, serial no. 10/290,650. However, as allowable subject matter has been indicated in neither this application nor the copending '650 application. Accordingly, the Examiner's rejection of Claims 1-63 is premature. Applicants will address substantively the Examiner's double-

patenting rejection when the Examiner indicates allowable subject matter in this application when the Examiner indicates that the claims in this application or the copending application are allowable.

Therefore, for the reasons set forth above, all pending claims (i.e., Claims 1-63) are allowable over the art of record. If the Examiner has any question regarding the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant at 408-392-9250.

Certificate of Transmission: I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office (USPTO) via the USPTO's electronic filing system on May 21, 2008.

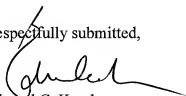


Attorney for Applicant(s)



Date of Signature

Respectfully submitted,



Edward C. Kwok  
Attorney for Applicant(s)  
Reg. No. 33,938

Law Offices of  
MacPherson Kwok Chen & Heid LLP  
2033 Gateway Place, Suite 400  
San Jose, CA 95110  
Tel: (408) 392-9250  
Fax: (408) 392-9262